WHAT IS CLAIMED IS:

1. A method of signing digital data, comprising the steps of:

subjecting the data to be signed to a message digest function to produce a digest of the data to be signed;

transmitting the message digest to a small, mobile transaction device which contains a secret key and a user's PIN code;

determining whether a user's PIN code is correct and, if it is, hashing the digest as a function of said secret key;

returning the transformed message digest to a service provider;

digesting and hashing the original data at the service provider using the same message digest function and secret key; and

determining whether the hashed message digest at the service provider matches the hashed message digest received from the transaction device.